ransomware.org
understand • prevent • recover

BY ActualTech Media

Running a Ransomware Tabletop Exercise

Most organizations are not prepared for a ransomware attack. With attacks on the rise, the need for companies to anticipate if, and when, they will fall victim to an attack is of utmost importance.

There seems to be a huge disconnect between the ransomware knowledge among IT security team members and what the rest of the company knows. One way to close that gap in knowledge is by engaging in **Tabletop Exercises. Tabletop Exercises help test your organization's Incident Response (IR) and Disaster Recovery (DR) plans.**

GOALS OF THE TABLETOP EXERCISE

Raising awareness is only one goal of a Ransomware Tabletop Exercise. In addition, organizations should plan to:

- ✓ **Test the assumptions and effectiveness of the company's IR and DR plans.**
- ✓ **Test the organization's interaction with the DR plan.**
- ✓ **Test the cybersecurity team's escalation and response procedures.**
- ✓ **Identify and fix gaps in processes.**

> **Tip:** Start with a trial run with a small core group and then follow that with an exercise including a larger group. It will help the actual exercise run smoother and you will have already mapped out basic assumptions.

WHO SHOULD ATTEND?

Departments that have a critical role in responding to a ransomware incident should be part of the Tabletop Exercise – from those dealing with actual cleanup to communication with employees, press, customers, and the attackers.

Representatives from the following departments should attend:

- Incident Response Team
- Each of the IT Teams
- Backups Team
- Every major office location
- Leadership
- Communications/Public Relations
- Human Resources
- Legal

> **Tip:** Reality is that people leave your organization. It's good to have two reps from each department to help ensure continuity.

ELEMENTS OF A SUCCESSFUL TABLETOP EXERCISE

1. **Appoint a facilitator to run the exercise and a note taker to document decisions and results.**
2. **Create a realistic Ransomware Response plan.**
3. **Test the Security Team's ability to respond to a ransomware attack.**
4. **Provide follow up tasks with owners and assignments. Include timelines for completion and follow up. Rank tasks by priority level.**
5. **Don't call out negatives on specific teams – make notes on the gaps in the plan.**
6. **Make everyone feel empowered by understanding what is working well and what needs improvement.**
7. **Create a fun and relaxed atmosphere. Encourage open minds to new ideas and feedback, and bring in good (catered!) food to keep people happy and alert.**

FINAL TIPS

Keep copies of your plan on different servers as well as (GASP!) in print.

Check your IR and DR plans annually as ransomware attacks change, and conduct a new Tabletop Exercise if changes are made.

Want more ransomware information? Go to ransomware.org >